constructed using any network fitting in the scope of OSI. The message transfer service provided by the MTS is application independent. An example of a standardized application is the IPM service. End systems can use the Message Transfer (MT) service for specific applications that are defined bilaterally.

Message handling services provided by Administrations belong to the group of telematic services defined in F.-Series Recommendations.

Various telematic services and telex (see Recommendations F.60, F.160, F.200, F.300, etc.), data transmission services (see Recommendation X.1), or physical delivery services (see Recommendation F.415) gain access to, and intercommunicate with, the IPM service or intercommunicate with each other, via access units.

Elements of service are the service features provided through the application processes. The elements of service are considered to be components of the services provided to users and are either elements of a basic service or they are *optional user facilities*, classified either as *essential optional user facilities*, or as *additional optional user facilities*.

7 Functional model of MHS

The MHS functional model serves as a tool to aid in the development of Recommendations for MHS, and aids in describing the basic concepts that can be depicted graphically. It comprises several different functional components that work together to provide MH services. The model can be applied to a number of different physical and organizational configurations.

7.1 *Description of the MHS model*

A functional view of the MHS model is shown in Figure 1/F.400. In this model, a user is either a person or a computer process. Users are either direct users (i.e. engage in message handling by direct use of MHS), or are indirect users [i.e. engage in message handling through another communication system (e.g. a physical delivery system) that is linked to MHS]. A user is referred to as either an originator (when sending a message) or a recipient (when receiving a message). Message handling elements of service define the set of message types and the capabilities that enable an originator to transfer messages of those types to one or more recipients.

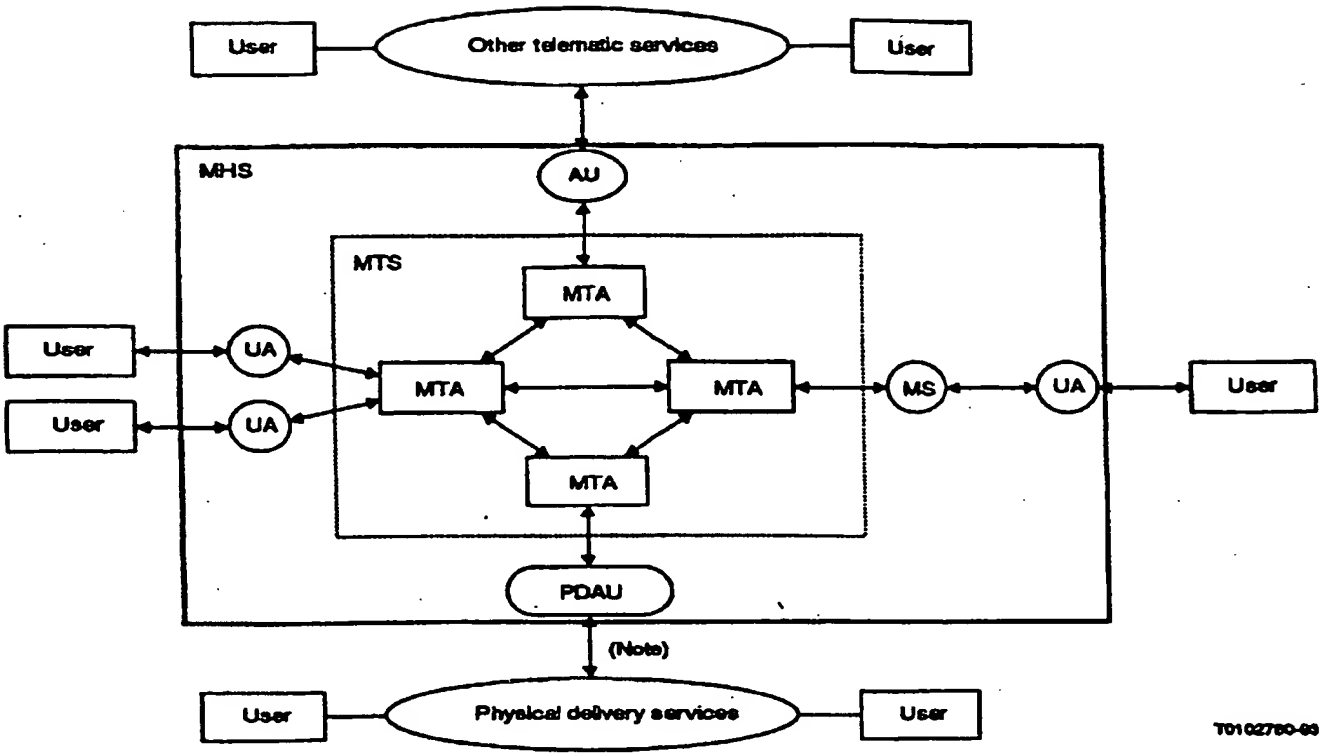
An originator prepares messages with the assistance of his user agent. A user agent (UA) is an application process that interacts with the message transfer system (MTS) or a message store (MS), to submit messages on behalf of a single user. The MTS delivers the messages submitted to it, to one or more recipient UAs, access units (AUs), or MSs, and can return notifications to the originator. Functions performed solely by the UA and not standardized as part of the message handling elements of service are called local functions. A UA can accept delivery of messages directly from the MTS, or it can use the capabilities of a MS to receive delivered messages for subsequent retrieval by the UA.

The MTS comprises a number of message transfer agents (MTAs). Operating together, in a store and forward manner, the MTAs transfer messages and deliver them to the intended recipients.

Access by indirect users of MHS is accomplished by AUs. Delivery to indirect users of MHS is accomplished by AUs, such as in the case of physical delivery, by the physical delivery access unit (PDAU).

The message store (MS) is an optional general purpose capability of MHS that acts as an intermediary between the UA and the MTA. The MS is depicted in the MHS functional model shown in Figure 1/F.400. The MS is a functional entity whose primary purpose is to store and permit retrieval of delivered messages. The MS also allows for submission from, and alerting to, the UA.

The collection of UAs, MSs, AUs and MTAs is called the message handling system (MHS).



Note – Message input from PDS to MHS is for further study. Flow from PD services to the PDAU shown is for the purpose of notifications.

FIGURE 1/F.400

MHS functional model

7.2 *Structure of messages*

The basic structure of messages conveyed by the MTS is shown in Figure 2/F.400. A message is made up of an envelope and a content. The envelope carries information that is used by the MTS when transferring the message within the MTS. The content is the piece of information that the originating UA wishes delivered to one or more recipient UAs. The MTS neither modifies or examines the content, except for conversion (see § 16).

7.3 *Application of the MHS model*

7.3.1 *Physical mapping*

Users access UAs for message processing purposes, for example, to create, present, or file messages. A user can interact with a UA via an input/output (I/O) device or process (e.g. keyboard, display, printer etc.). A UA can be implemented as a (set of) computer process(es) in an intelligent terminal.

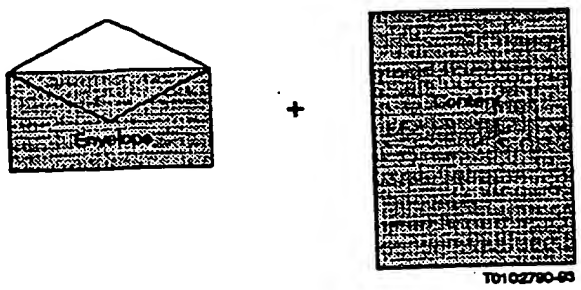


FIGURE 2/F.400
Basic message structure

A UA and MTA can be co-located in the same system, or a UA/MS can be implemented in physically separate systems. In the first case the UA accesses the MT elements of service by interacting directly with the MTA in the same system. In the second case, the UA/MS will communicate with the MTA via standardized protocols specified for MHS. It is also possible for an MTA to be implemented in a system without UAs or MSs.

Some possible physical configurations are shown in Figures 3/F.400 and 4/F.400. The different physical systems can be connected by means of dedicated lines or switched network connections.

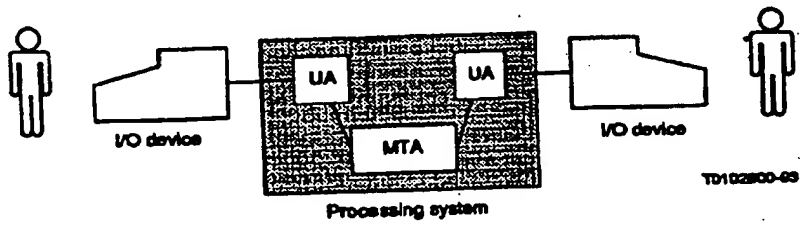


FIGURE 3/F.400
Co-resident UA and MTA

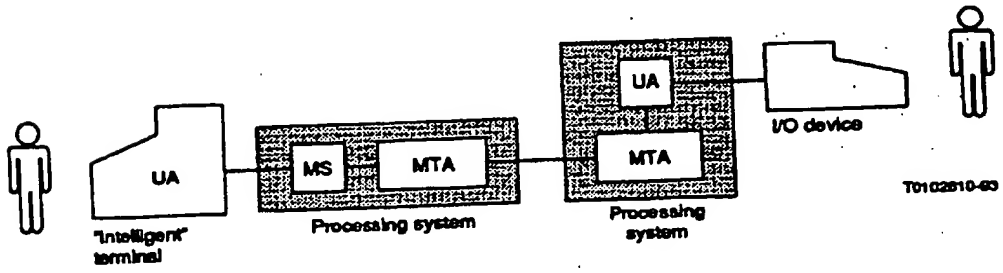


FIGURE 4/F.400
Stand-alone UA and co-resident MS/MTA and UA/MTA

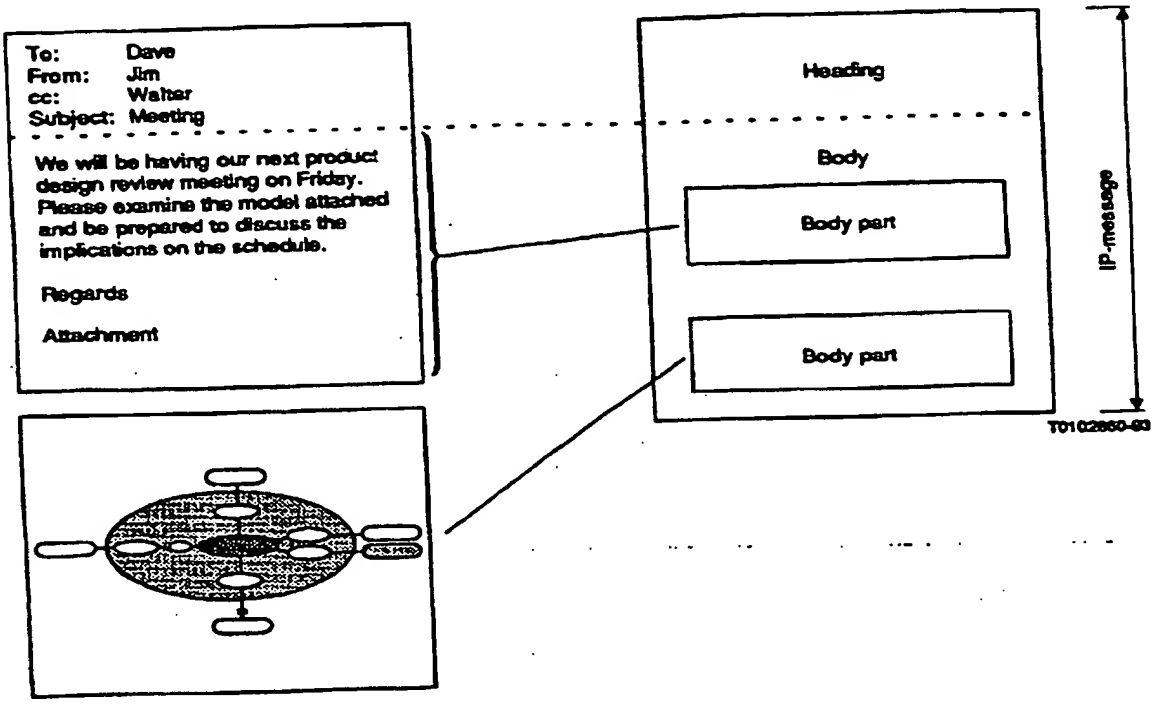


FIGURE 9/F.400

IP-message structure for a typical memo

10 Intercommunication with physical delivery services

10.1 *Introduction*

The value of message handling systems can be increased by connecting them to physical delivery (PD) systems such as the traditional postal service. This will allow for the physical (e.g. hardcopy) delivery of messages originated within MHS to recipients outside of MHS, and in some cases will allow for the return of notifications from the PD service to an MHS originator. The ability for origination of messages in the PD service for submission to MHS through the PDAU is for further study. The capability of intercommunication between PD and MH services is an optional capability of MHS, and is applicable to any application such as IPM. All users of MHS will have the ability to generate messages for subsequent physical delivery. Figure 10/F.400 shows the functional model of this interworking. Provision of intercommunication between public message handling services offered by Administrations and PD services is described in Recommendation F.415. The elements of service describing the features of this intercommunication are defined in Annex B and classified in § 19.

A physical delivery system is a system, operated by a management domain, that transports and delivers physical messages. A physical message is a physical object comprising a relaying envelope and its content. An example of a physical delivery system (PDS) is the postal service. An example of a physical message is a paper letter and its enclosing paper envelope.

A physical delivery access unit (PDAU) converts an MH user's message to physical form, a process called physical rendition. An example of this is the printing of a message and its automatic enclosure in a paper envelope. The PDAU passes the physically rendered message to a PDS for further relaying and eventual physical delivery.

A PDAU can be viewed as a set of UAs, each UA being identified by a postal address. To perform its functions, a PDAU must support submission (Notifications) and delivery interactions with the MTS, and also cooperate with other UAs. MH/PD service intercommunication is thus provided as part of the message transfer service.

To enable MH users to address messages to be delivered physically by a PDS, an appropriate address format is described in § 12.

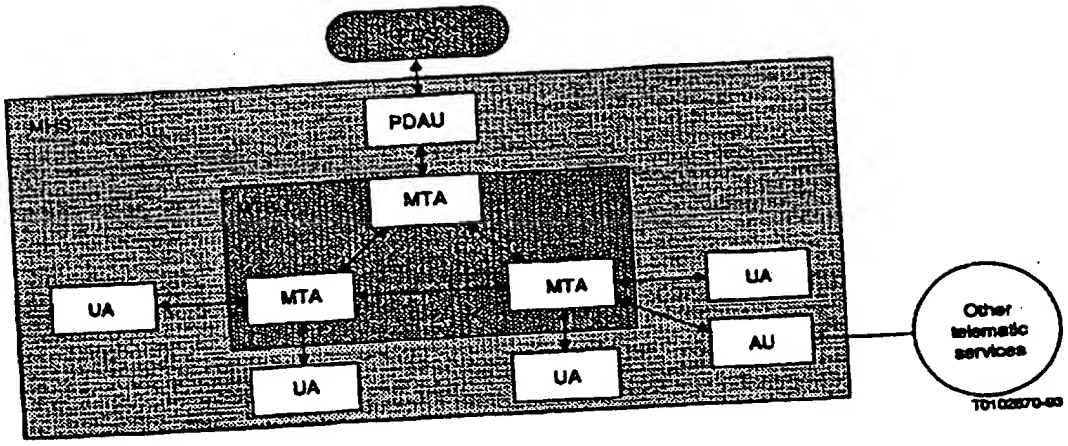


FIGURE 10/F.400

Functional model MHS-PDS interworking

10.2 *Organizational configurations*

Possible organizational mappings of the functional model described above are shown in Figure 11/F.400. In each model (A and B), the term PD domain denotes the domain of responsibility of an organization providing a PD service. In A, the PD domain comprises an MD and a PDS. The boundary between the PD domain and the rest of MHS is a boundary between MDs. In B, the PD domain comprises only the PDS; the PDAU is not part of the PD domain. The boundary between the PD domain and MHS lies at the point where the PDAU passes physical messages to the PDS.

11 Specialized access

11.1 *Introduction*

The functional model of MHS (see Figure 1/F.400) contains access units (AUs) to allow access between MHS and other communication systems and services. The model shows a generic access unit between MHS and telematic services.

Also shown is a physical delivery access unit to allow for physical delivery of MHS messages to recipients without the need for terminal access to MHS. The access to physical delivery services is available to any application carried by the MTS, through a PDAU described in § 10.

Other forms of access are described below.

The capabilities in this section cover the application of security features to protect messages directly submitted to the message transfer system by a user agent, message store, or an access unit. They do not cover the application of security features to protect communication between users and the message handling system, or MH user-to-MH user communication (a large part of MH user-to-MH user communication is protected between two UAs). Thus they do not apply, for example, to communication between a remote user's terminal and its UA, or to communication between these users' terminal equipment and other users in the MHS. Security capabilities to protect MH user-to-MH user communication are for further study.

Many of the secure messaging elements of service provide an originator-to-recipient capability, and require the use of user agents with security capabilities. They do not require the use of a message transfer system with security features. [As an example, content confidentiality can be applied by enciphering the message content by the originator, and deciphering by the recipient, with various security parameters transferred within the message envelope. Such a message can be transferred by any MTS which can handle the format of the content (unformatted octets), and transparently handle the security fields in the envelope.]

Some of the secure messaging elements of service involve an interaction with the Message transfer system, and require the use of message transfer agents with security capabilities. (As an example, non-repudiation of submission requires the MTA, to which the message is submitted, to contain mechanisms to generate a proof of submission field.)

Some of the secure messaging elements of service apply to the MS as well as UAs and MTAs, such as message security labelling. In general, however, the MS is transparent to security features that apply between the originators' and the recipients's UAs.

The scope of the secure messaging elements of service is given in Table 2/F.400. This describes the elements of service in terms of which the MHS component is the "provider" or the "user" of the security service. For example, probe-origin authentication is provided by the originating UA, and can be used by the MTAs through which the probe passes. An overview of these elements of service is given in § 15.4.

This overview describes the use of security services by the UA, MS, and the MTA. How these features are applied to access units is for further study.

15.4 *MHS-security capabilities*

The elements of service describing the security features of MHS are defined in Annex B, and classified in § 19. An overview of these capabilities is as follows:

- *Message origin authentication:* Enables the recipient, or any MTA through which the message passes, to authenticate the identity of the originator of a message.
- *Report origin authentication:* Allows the originator to authenticate the origin of a delivery/non-delivery report.
- *Probe origin authentication:* Enables any MTA through which the probe passes, to authenticate the origin of the probe.
- *Proof of delivery:* Enables the originator of a message to authenticate the delivered message and its content, and the identity of the recipient(s).
- *Proof of submission:* Enables the originator of a message to authenticate that the message was submitted to the MTS for delivery to the originally specified recipient(s).
- *Secure access management:* Provides for authentication between adjacent components, and the setting up of the security context.
- *Content integrity:* Enables the recipient to verify that the original content of a message has not been modified.
- *Content confidentiality:* Prevents the unauthorized disclosure of the content of a message to a party other than the intended recipient.
- *Message flow confidentiality:* Allows the originator of a message to conceal the message flow through MHS.

- *Message sequence integrity:* Allows the originator to provide to a recipient proof that the sequence of messages has been preserved.
- *Non-repudiation of origin:* Provides the recipient(s) of a message with proof of origin of the message and its content which will protect against any attempt by the originator to falsely deny sending the message or its content.
- *Non-repudiation of delivery:* Provides the originator of a message with proof of delivery of the message which will protect against any attempt by the recipient(s) to falsely deny receiving the message of its content.
- *Non-repudiation of submission:* Provides the originator of a message with proof of submission of the message, which will protect against any attempt by the MTS to falsely deny that the message was submitted for delivery to the originally specified recipient(s).
- *Message security labelling:* Provides a capability to categorize a message, indicating its sensitivity, which determines the handling of a message in line with the security policy in force.

TABLE 2/F.400

Provision and use of secure messaging elements of service by MHS components

Elements of service	Originating MTS user	MTS	Recipient MTS user
Message origin authentication	P	U	U
Report origin authentication	U	P	–
Probe origin authentication	P	U	–
Proof of delivery	U	–	P
Proof of submission	U	P	–
Secure access management	P	U	P
Content integrity	P	–	U
Content confidentiality	P	–	U
Message flow confidentiality	P	–	–
Message sequence integrity	P	–	U
Non-repudiation of origin	P	–	U
Non-repudiation of submission	U	P	–
Non-repudiation of delivery	U	–	P
Message security labelling	P	U	U

P The MHS component is a provider of the service.

U The MHS component is a user of the service.

15.5 *Security management*

Aspects of an asymmetric key management scheme to support the above features are provided by the directory system authentication framework, described in CCITT Rec. X.509 | ISO/IEC 9594-8. The Directory stores certified copies of public keys for MH users which can be used to provide authentication and to facilitate key exchange for use in data confidentiality and data integrity mechanisms. The certificates can be read from the Directory using the directory access protocol described in CCITT Rec. X.519 | ISO/IEC 9594-5.

Other types of key management schemes, including symmetric encryption, to support the security features are for further study.

15.6 *MHS-security dependencies*

If, as a result of using MHS security capabilities, there are any dependencies, consequences or restrictions on other MHS capabilities (e.g. on distribution lists or conversion), then these shall be defined by the security policy.

The abstract security model for message transfer is described in § 10 of Recommendation X.402. In particular, § 10.1 of Recommendation X.402 describes the concept of security policy.

16 Conversion in MHS

The MTS provides conversion functions to allow users to input messages in one or more encoded formats, called encoded information types (EITs), and have them delivered in other EITs to cater to users with various UA capabilities and terminal types. This capability is inherent in the MTS and increases the possibility of delivery by tailoring the message to the recipient's terminal capabilities. The EITs standardized in MHS are listed in CCITT Rec. X.411 | ISO/IEC 10021-4. Conversions and the use of the elements of service relating to conversion are available for EITs not defined in CCITT Rec. X.411 | ISO/IEC 10021-4, but supported by certain domains, either bilaterally between these domains or within a domain itself.

MH users have some control over the conversion process through various elements of service as described in Annex B. These include the ability for a user to explicitly request the conversion required or as a default to let the MTS determine the need for conversion, and the type of conversion performed. Users also have the ability to request that conversion not be performed or that conversion not be performed if loss of information will result. When the MTS performs conversion on a message, it informs the UA to whom the message is delivered that conversion took place and what the original EITs were.

17 Use of the MHS in provision of public services

The message handling system is used in the provision of public MH services that are offered by Administrations for use by their subscribers. These public MH services are defined in the F.400-Series of Recommendations and include:

- the public message transfer service (Recommendation F.410);
- the public interpersonal messaging service (Recommendation F.420).

In addition, complementary public services are offered by Administrations to allow for the intercommunication between CCITT services and the public MH services mentioned above, as follows:

- intercommunication between the IPM service and the telex service (Recommendation F.421);
- intercommunication between the IPM service and the teletex service (Recommendation F.422);
- intercommunication between the IPM service and telefax services (Recommendation F.423);
- intercommunication with public physical delivery services (Recommendation F.415);

A Recommendation describing the naming and addressing aspects for public MH services exists as follows:

- naming and addressing for public message handling services (Recommendation F.401).

See also Recommendations F.435 and F.440.

18 Elements of service – Purpose

Elements of service are particular features, functions, or capabilities of MHS. All the elements of service applicable for MHS are defined in Annex B, where they are listed in alphabetical order with a corresponding reference number. The realization of these elements of service in MHS are described in other CCITT Recommendations in the X.400 series | parts of ISO/IEC 10021.

Elements of service are associated with the various services provided in MHS. There are elements of service for the message transfer service which provide for a basic capability for sending and receiving messages between UAs. There are elements of service for the interpersonal messaging service which provide for the sending and receiving of messages between a particular class of UAs called IPM UAs. There are elements of service for the physical delivery service, enabling MH users to send messages and have them delivered in a physical medium to non-MH users. There are elements of service specifically available for the use of message stores.

The elements of service for the IPM service include those available for the MT service, the PD service, and the message store as well as specific ones applicable to the IPM service.

Table 3/F.400 lists all the elements of service available in MHS except those defined in Recommendations. F.435 and F.440, shows what service they are specifically associated with of the presently defined services, MT service, IPM service, and PD service, or whether they are specific to the message store, and gives the corresponding reference number to the definition in Annex B.

TABLE 3/F.400

MHS elements of service

Elements of service	MT	IPM	PD	MS	Annex B reference
Access management	X		X		B.1
Additional physical rendition					B.2
Alternate recipient allowed	X				B.3
Alternate recipient assignment	X				B.4
Authorizing users indication		X			B.5
Auto-forwarded indication		X			B.6
Auto-submitted indication		X			B.94
Basic physical rendition			X		B.7
Blind copy recipient indication		X			B.8
Body part encryption indication		X			B.9
Content confidentiality	X				B.10
Content integrity	X				B.11
Content type indication	X				B.12
Conversion prohibition	X				B.13
Conversion prohibition in case of loss of information	X				B.14
Converted indication	X				B.15
Counter collection			X		B.16
Counter collection with advice			X		B.17
Cross-referencing indication		X			B.18
Deferred delivery	X				B.19
Deferred delivery cancellation	X				B.20
Delivery notification	X				B.21
Delivery time stamp indication	X				B.22
Delivery via bureaufax service			X		B.23
Designation of recipient by directory name	X				B.24
Disclosure of other recipients	X				B.25
DL-expansion history indication	X				B.26
DL-expansion prohibited	X				B.27
EMS (express mail service)			X		B.28
Expiry date indication		X			B.29
Explicit conversion	X				B.30

TABLE 3/F.400 *(cont.)*

Elements of service	MT	IPM	PD	MS	Annex B reference
Forwarded IP-message indication		X			B.31
Grade of delivery selection	X				B.32
Hold for delivery	X				B.33
Implicit conversion	X				B.34
Importance indication		X			B.35
Incomplete copy indication		X			B.36
IP-message identification		X			B.37
Language indication		X			B.38
Latest delivery designation	X				B.39
Message flow confidentiality	X				B.40
Message identification	X				B.41
Message origin authentication	X				B.42
Message security labelling	X				B.43
Message sequence integrity	X				B.44
MS register				X	B.95
Multi-destination delivery	X				B.45
Multi-part body		X			B.46
Non-delivery notification	X				B.47
Non-receipt notification request indication		X			B.48
Non-repudiation of delivery	X				B.49
Non-repudiation of origin	X				B.50
Non-repudiation of submission	X				B.51
Obsoleting indication		X			B.52
Ordinary mail			X		B.53
Original encoded information types indication	X				B.54
Originator indication		X			B.55
Originator requested alternate recipient	X				B.56
Physical delivery notification by MHS			X		B.57
Physical delivery notification by PDS			X		B.58
Physical forwarding allowed			X		B.59
Physical forwarding prohibited			X		B.60
Prevention of non-delivery notification	X				B.61
Primary and copy recipients indication		X			B.62
Probe	X				B.63
Probe origin authentication	X				B.64
Proof of delivery	X				B.65
Proof of submission	X				B.66
Receipt notification request indication		X			B.67
Redirection disallowed by originator	X				B.68
Redirection of incoming messages	X				B.69
Registered mail			X		B.70
Registered mail to addressee in person			X		B.71
Reply request indication		X			B.72
Replying IP-message indication		X			B.73
Report origin authentication	X				B.74
Request for forwarding address			X		B.75
Requested preferred delivery method	X				B.76
Restricted delivery	X				B.77
Return of content	X				B.78
Secure access management	X				B.79
Sensitivity indication		X			B.80